Éthique numérique et données de santé

Module 8 — Programme Devenir infirmier — les fondamentaux

UE A.2 · D.4 · Semestre 1

Référentiel IDE · Arrêté 20/02/2026

Données de santé — RGPD Art. 9

- Catégorie spéciale de données — protection renforcée
- Hébergement obligatoire sur serveur certifié HDS (Hébergeur Agréé Données de Santé)
- Durée de conservation dossier médical : 20 ans minimum
- Notification CNIL en cas de violation : 72h maximum
- 5 traits identitovigilance : nom de naissance + prénom + DDN + sexe + INS

⚠ Interdit — s'applique dès le 1er stage

- ✗ Photo d'un patient sans consentement écrit explicite
- ✗ Données de santé sur téléphone perso ou Gmail
- ✗ Données sur WhatsApp / Signal / Google Drive (non HDS)
- ✗ Données patient dans un outil d'IA grand public
- ✗ Utiliser la session d'un collègue
- ✗ Partager son mot de passe (à personne, jamais)
- ✗ Accéder au DPI d'un patient dont vous n'avez pas la charge

CYBERSÉCURITÉ — 4 RÈGLES FONDAMENTALES

Mot de passe

Unique, complexe, non partagé — jamais communiqué même à un collègue.

Violation → responsabilité engagée

Session

Verrouiller dès que vous quittez un poste, même 30 secondes. Actes tracés sous votre identifiant.

Session ouverte = responsabilité

Phishing

Email demandant identifiants = phishing. Ne jamais cliquer ni répondre. Signaler au service info.

Signalement immédiat obligatoire

Supports externes

Clé USB inconnue interdite sur postes hospitaliers. Vecteur d'infection malware.

Refus systématique

Incident de sécurité → signalement immédiat au responsable informatique. Ne pas éteindre le poste sans instruction.

OUTILS NUMÉRIQUES CLÉS À CONNAÎTRE EN STAGE

Outil	Définition	Règle clé
DPI — Dossier patient informatisé	Traçabilité et continuité des soins en établissement. Chaque accès journalisé avec votre identifiant.	Accès limité aux patients dont vous avez la charge
DMP — Dossier médical partagé	Dossier de santé transversal du patient, accessible à tous les professionnels autorisés par lui.	Le patient contrôle les accès
MSSanté	Messagerie sécurisée de santé entre professionnels. Alternative légale à WhatsApp/email non sécurisé.	À utiliser pour tout échange sur un patient
CPS — Carte professionnelle de santé	Authentification forte pour accès aux systèmes de santé sécurisés. Identité professionnelle numérique.	Ne jamais prêter, ne jamais partager le code PIN

IA EN SANTÉ — POSTURE PROFESSIONNELLE

L'IA apporte

Détection de signaux faibles, aide au diagnostic, alertes prédictives (chute, sepsis), aide à la rédaction, coordination des soins.

L'IA ne remplace pas

Votre jugement clinique, la relation soignant-soigné, le contexte humain, votre responsabilité professionnelle.

Alerte IA = signal à intégrer dans l'évaluation clinique. Réévaluer, documenter, informer. Ne jamais appliquer mécaniquement ni ignorer.

TÉLÉSANTÉ — CADRE LÉGAL (LOI 24/07/2019)

Téléconsultation : consultation à distance patient-professionnel

Télésoin infirmier : ETP, suivi chronique, post-hosp. à distance

Télésurveillance : suivi via objets connectés (glycémie, ECG, TA)

Téléexpertise : avis spécialiste à distance pour un professionnel

POINTS CLÉS

- Données de santé = catégorie spéciale RGPD — hébergement HDS obligatoire, jamais sur outil non agréé.
- Identitovigilance : 5 traits stricts — nom naissance, prénom, DDN, sexe, INS.
- Session verrouillée = actes tracés sous votre identifiant. Jamais de session tierce.
- Mot de passe = strictement personnel. Ne se partage jamais, à personne.
- DPI ≠ DMP : DPI = interne à l'établissement, DMP = transversal contrôlé par le patient.
- L'IA assiste le jugement clinique — elle ne le remplace pas et ne décharge pas votre responsabilité.
- Phishing = ne jamais cliquer, ne jamais répondre, signaler immédiatement au service informatique.